МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н.Ельцина»

УТВЕРЖДАЮ:
Проректор по учебной работе

_____ С.Т. Князев

«___» _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Образовательная программа **Экономическая безопасность**	Код ОП 38.05.01/01.02
Направление подготовки **Экономическая безопасность**	Код направления и уровня подготовки ***38.05.01***
Уровень подготовки **Специалитет**	
ФГОС ВО	Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО *от 16.01.2017 г. № 20*

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Акбердина В.В.	Д.э.н, проф.	профессор	Региональной экономики, инновационного предпринимательства и безопасности	
2	Крылов В.Г.		доцент	Региональной экономики, инновационного предпринимательства и безопасности	

Рекомендовано учебно-методическим советом института государственного управления и предпринимательства

Председатель учебно-методического совета А.А. Яшин
Протокол № 6 от 22 февраля 2017 г.

Согласовано:

Дирекция образовательных программ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ Информационная безопасность

1.1.Аннотация содержания дисциплины

Дисциплина «Информационная безопасность» является дисциплиной вариативной части учебного плана. Содержание дисциплины охватывает круг вопросов, направленных на изучение информационных технологий для анализа информации и поддержки принятия управленческих решений, технологии защиты информации, web-технологии, технологии управления проектами и работы со специализированным прикладным программным обеспечением при ведении управленческой деятельности.

Дисциплина «Информационная безопасность» занимает важное место в структуре образования и подготовки будущих специалистов экономической безопасности. Теоретической основой дисциплины «Информационная безопасность» являются основные положения дисциплин математики и информатики в объемах базовых курсов. В рамках курса «Информационная безопасность» применяются такие методы преподавания как проблемные лекции с использованием информационного поиска в сети Интернет, анализ конкретных ситуаций. Для успешного освоения курса студентам рекомендуется ознакомиться с содержанием статей в научных журналах, отчетами о научно-исследовательской работе, сайтами научных организаций в сети Интернете, электронным каталогом диссертаций, авторефератами диссертаций, материалами научных конференций.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Изучение дисциплины направлено на освоение студентами следующих компетенций:

способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12);

способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач (ПК-28);

способность проводить анализ и давать оценку возможных экономических рисков, составлять и обосновывать прогнозы динамики развития основных угроз экономической безопасности (ПК-32);

способностью анализировать эмпирическую и научную информацию, отечественный и зарубежный опыт по проблемам обеспечения экономической безопасности (ПК-45);

способностью исследовать условия функционирования экономических систем и объектов, формулировать проблемы, обосновывать актуальность и практическую значимость разрабатываемых мероприятий по обеспечению экономической безопасности, методов и средств анализа экономической безопасности организаций, оценивать их эффективность (ПК-46);

способностью проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации (ПК-48);

способностью готовить отчеты, справки и доклады по результатам выполненных исследований (ПК-49);

Цели изучения дисциплины:

- формирование у студентов методически правильных основ знаний в сфере информационной безопасности;
- ознакомление студентов с нормативной, законодательной базой по информационной безопасности;
- ознакомление студентов с современными методами, средствами и системами обеспечения информационной безопасности;
- развитие навыков применения средств защиты информации при использовании информационных технологий;
- обучение методам работы со встроенными механизмами безопасности популярных программных пакетов;

В результате освоения дисциплины студент должен:

Знать:

- основные угрозы безопасности при использовании информационных технологий;
- меры ответственности за нарушение информационной безопасности;
- назначение различных средств и систем защиты информации;
- средства безопасности современных операционных систем;
- способы защиты информации.
- основы криптографических мер защиты информации;
- организационные меры по защите информации.

Уметь:

- определять основные угрозы безопасности при использовании информационных технологий;
- производить мониторинг безопасности информационных систем;
- применить полученные знания в процессе дальнейшего обучения и своей профессиональной деятельности.

Владеть (демонстрировать навыки и опыт деятельности):

- навыками выявления нарушений информационной безопасности;
- навыками работы со встроенными средствами безопасности операционных систем и офисного программного обеспечения;
- навыками безопасной работы в глобальных и локальных информационных сетях.

1.4. Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	7
1.	Аудиторные занятия	68	68	68
2.	Лекции	17	17	17
3.	Практические занятия	51	51	51
4.	Лабораторные работы			
5.	Самостоятельная работа студентов, включая все виды текущей аттестации	58	10,20	58
6.	Промежуточная аттестация	Э (18)	2,33	Э (18)
7.	Общий объем по учебному плану, час.	144	80,53	144
8.	Общий объем по учебному плану, з.е.	4		4

Заочная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины	Распределение объема дисциплины по семестрам (час.)

		Всего часов	В т.ч. контактная работа (час.)*	9
1.	Аудиторные занятия	14	14	14
2.	Лекции	4	4	4
3.	Практические занятия	10	10	10
4.	Лабораторные работы			
5.	Самостоятельная работа студентов, включая все виды текущей аттестации	112	2,10	112
6.	Промежуточная аттестация	Э (18)	2,33	Э (18)
7.	Общий объем по учебному плану, час.	144	18,43	144
8.	Общий объем по учебному плану, з.е.	4		4

Заочная (ускоренная) форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)	
		Всего часов	В т.ч. контактная работа (час.)*	4	5
1.	Аудиторные занятия	6	6	2	4
2.	Лекции	2	2	2	
3.	Практические занятия	4	4		4
4.	Лабораторные работы				
5.	Самостоятельная работа студентов, включая все виды текущей аттестации	48	0,90	34	14
6.	Переаттестация, час (з.е)	72 (2)		72 (2)	
7.	Промежуточная аттестация	Э (18)	2,33		Э (18)
8.	Общий объем по учебному плану, час.	144	6,23	36	36
9.	Общий объем по учебному плану, з.е.	4		3	1

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Введение	Определение понятия “информационная безопасность”. Информационная безопасность как отрасль. Роль и место информационной безопасности в профессиональной деятельности. Современное состояние и перспективы информаци-

Код раздела, темы	Раздел, тема дисциплины*	Содержание
		онной безопасности. Государственное регулирование в сфере ИБ. Международные нормы и стандарты по ИБ.
Р2	Виды угроз ИБ	Классификация угроз информации и информационным технологиям. Субъекты ИБ. Угрозы доступности, целостности и конфиденциальности информации. Категории атак на информационные системы. Сценарий типовой атаки на информационную систему. Локальные атаки. Удаленные атаки. Атаки на поток данных. Атаки на пользователя (социальная инженерия).
Р3	Безопасность программного обеспечения	Средства защиты информации и обеспечения безопасности информационных технологий. Определение понятия «уязвимость программного обеспечения». Обзор методик тестирования и выявления уязвимостей. Организационные меры по обеспечению безопасности использования программного обеспечения. Меры защиты и подтверждения авторских прав на разрабатываемое программное обеспечение.
Р4	Встроенные средства безопасности операционных систем	Средства идентификации и аутентификации пользователей. Группы безопасности. Политика регистрации событий. Шифрование. Корпоративная безопасность. Службы сертификации. Встроенный Firewall. Политика ограничения используемых приложений. Средства электронной цифровой подписи. Защита от макровирусов. Централизованные средства управления. Компьютерные вирусы и антивирусные средства. Антивирусное программное обеспечение (АВПО). Обзор технологий и производителей АВПО. Практика применения АВПО. Эшелонированные системы антивирусной защиты. Атаки на АВПО.
Р5	Криптографические методы защиты информации	Шифрование (алгоритмы шифрования). Электронно-цифровая подпись (практика применения). Хэширование. Средства инфраструктуры открытых ключей. Атаки на криптографическую защиту.
Р6	Сетевые средств защиты информации.	Технологии защиты вычислительных сетей. Обзор сетевых средств защиты информации (межсетевые экраны, виртуальные частные сети, шифрование, обнаружение вторжений). Методы применения сетевых СЗИ. Основы безопасной работы в сети Интернет. Безопасность электронной коммерции. Безопасность беспроводных технологий. Стандарты безопасности беспроводных сетей. Меры защиты от различного вида атак. Технологии защиты Wi-Fi-сетей.
Р7	Управление рисками ИБ	Соотношение угроз, уязвимостей и ущерба. Этапы управления рисками. Методики оценки рисков. Методы снижения рисков. Организация системы информационной безопасности предприятия. Построение системы управления информационной безопасности (СУИБ) предприятия. Общие правила безопасности предприятия. Архитектура СУИБ. Настройки основных компонентов СУИБ. Корпоративные политики информационной безопасности

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. *Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины*

Очная форма обучения

Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	Всего по разделу, теме (час.)	Всего аудиторной работы (час.)	Лекции	Практические занятия	Лабораторные работы	Всего самостоятельной работы студентов (час.)	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	Всего (час.)	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязычной литературы*	Курсовая работа*	Курсовой проект*	Всего (час.)	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Введение	**6**	**4**	1	3		**2**	**2**	1	1																				
Р2	Виды угроз ИБ	**22**	**8**	2	6		**14**	**4**	2	2			**10**	1																
Р3	Безопасность программного обеспечения	**18**	**12**	3	9		**6**	**6**	3	3																				
Р4	Встроенные средства безопасности операционных систем	**13**	**8**	2	6		**5**	**5**	2	3																				
Р5	Криптографические методы защиты информации	**25**	**16**	4	12		**9**	**9**	4	5																				
Р6	Сетевые средств защиты информации.	**20**	**12**	3	9		**8**	**8**	3	5																				
Р7	Управление рисками ИБ	**22**	**8**	2	6		**14**	**4**	2	2			**10**	1																
	Всего (час), без учета промежуточной аттестации**:**	**126**	**68**	**17**	**51**		**58**	**38**	**17**	**21**			**20**	**20**																
	Всего по дисциплине (час.):	**144**	**68**				**58**	В т.ч. промежуточная аттестация																			**0**	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

Заочная форма обучения

Объем дисциплины (зач.ед.):4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	Всего по разделу, теме (час.)	Всего аудиторной работы (час.)	Лекции	Практические занятия	Лабораторные работы	Всего самостоятельной работы студентов (час.)	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	Всего (час.)	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязы. литературы*	Курсовая работа*	Курсовой проект*	Всего (час.)	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Введение	12	2	1	1		10	10	4	6																				
Р2	Виды угроз ИБ	25	1		1		24	14	6	8			10	1																
Р3	Безопасность программного обеспечения	16	2		2		14	14	6	8																				
Р4	Встроенные средства безопасности операционных систем	16	2		2		14	14	6	8																				
Р5	Криптографические методы защиты информации	17	3	1	2		14	14	6	8																				
Р6	Сетевые средств защиты информации.	17	3	1	2		14	14	6	8																				
Р7	Управление рисками ИБ	23	1	1	-		22	12	6	6			10	1																
	Всего (час), без учета промежуточной аттестации**:**	126	14	4	10		112	92	40	52			20	20																
	Всего по дисциплине (час.):	144	14				112	В т.ч. промежуточная аттестация																				0	18	0	0

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

Заочная (ускоренная) форма обучения

Объем дисциплины (зач.ед.):4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	Всего по разделу, теме (час.)	Всего аудиторной работы (час.)	Лекции	Практические занятия	Лабораторные работы	Всего самостоятельной работы студентов (час.)	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)												Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	Всего (час.)	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязы. литературы*	Курсовая работа*	Курсовой проект*	Всего (час.)	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Введение	5	1	1			4	4	1	3																				
Р2	Виды угроз ИБ	13	-	-	-		13	3	1	2			**10**	1																
Р3	Безопасность программного обеспечения	6	1		1		5	5	2	3																				
Р4	Встроенные средства безопасности операционных систем	6	1		1		5	5	2	3																				
Р5	Криптографические методы защиты информации	6	1	1			5	5	2	3																				
Р6	Сетевые средств защиты информации.	4	1		1		3	3	1	2																				
Р7	Управление рисками ИБ	14	1		1		13	3	1	2			**10**	1																
	Всего (час), без учета промежуточной аттестации и переаттестации**:**	**54**	**6**	**2**	**4**		**48**	**28**	**10**	**18**			**20**	**20**																
	Переаттестация	**72**																												
	Всего по дисциплине (час.):	**144**						В т.ч. промежуточная аттестация																			**0**	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

Не предусмотрено

4.2. Практические занятия

Очная форма обучения

№	Раздел дисциплины	Тема занятия	Объем учебного времени, час.
1	Р1	Анализ нормативных документов и стандартов информационной безопасности.	3
2	Р2	Классификация угроз информации и информационным технологиям. Этичный хакинг.	6
3	Р3	Установка и управление антивирусным программным обес-	9
4	Р4	Установки локальной политики безопасности	6
5	Р5	Шифрование локальных документов. Операции с сертифи-	12
6	Р6	Настройка персонального межсетевого экран (брандмауэр, файрвол – Brandmauer, Firewall)	9
7	Р7	Анализ рисков по данным лог-файлов событий	6
		Итого:	51

Заочная форма обучения

№	Раздел дисциплины	Тема занятия	Объем учебного времени, час.
1	Р1	Анализ нормативных документов и стандартов информационной безопасности.	1
2	Р2	Классификация угроз информации и информационным технологиям. Этичный хакинг.	1
3	Р3	Установка и управление антивирусным программным	2
4	Р4	Установки локальной политики безопасности	2
5	Р5	Шифрование локальных документов. Операции с серти-	2
6	Р6	Настройка персонального межсетевого экран (брандмауэр, файрвол – Brandmauer, Firewall)	2
		Итого:	10

Ускоренная форма обучения

№	Раздел дисциплины	Тема занятия	Объем учебного времени, час.

1	Р3	Установка и управление антивирусным программным	1
2	Р4	Установки локальной политики безопасности	1
3	Р6	Настройка персонального межсетевого экран (брандмауэр, файрвол – Brandmauer, Firewall)	1
4	Р7	Анализ рисков по данным лог-файлов событий	1
		Итого:	4

4.3. Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

Студентам предлагается подготовить и сделать доклад (в виде презентации) по выбранной теме. Объем работы задается временем, отводимым на презентацию – до 10 минут.

Домашняя работа 1

1. Криптографические средства защиты информации в стандарте GSM и их стойкость.
2. Исследование алгоритма поточного шифрования RC4.
3. Особенности применения цифровой подписи вслепую в протоколах электронного тайного голосования.
4. Новые американские стандарты режимов шифрования с аутентификацией.
5. Схемы криптосистем на основе парных отображений.
6. Методы эффективной реализации схем электронной цифровой подписи на основе группы точек эллиптических кривых.
7. Возможности преобразования отечественного стандарта цифровой подписи в схему цифровой подписи вслепую.
8. Сравнение криптографических средств различных протоколов мобильных платежей.
9. Исследование свойств подстановок на двоичных векторах при малых размерностях и их применение при построении узлов алгоритмов шифрования.
10. Решение проблемы повторной траты (https://ru.wikipedia.org/wiki/Двойное_расходование) криптографическими методами в схемах электронных платежей.
11. Анализ подходов к ролевому управлению доступом
12. Аудит безопасности информационной системы с использованием теста на проникновение
13. Аудит информационной безопасности
14. Выявление нарушений законодательства в сети Интернет
15. Выявление признаков, определяющих группы по интересам
16. Шифрование информации. Цель, место, применение
17. Защита информации предприятия от утечки по техническим каналам
18. Защита конфиденциальной информации на предприятиях по формам собственности
19. Защита персональных данных на предприятиях
20. Криптографические методы защиты информации
21. Криптоанализ алгоритмов: Hughes XPD/KPD, Nanoteq
22. Криптоанализ генераторов: «стоп-пошёл» Both-Piper, DNRSG, Геффа, Дженнингса,каскад Голлманна
23. Криптоанализ потоковых шифров: Gifford, A5, LFSR

Домашняя работа 2

1. Защита информационной и интеллектуальной собственности
2. Информационные угрозы предпринимательству
3. Исследование проблем информационной безопасности и защита информации территориально разнесенных центров обработки данных
4. Исследование проблем информационной безопасности мобильного доступа

5. Исследование тенденций развития межсетевых экранов прикладного уровня
6. Линейная сложность генераторов на базе LFSR
7. Место DLP-систем (предотвращение утечек, Data Leak Prevention) в современной структуре обеспечения информационной безопасности автоматизированной информационной системы
8. Оценка рисков информационной безопасности при обеспечении доступа в Интернет
9. Защита информации в облачных сервисах
10. Организационно-правовое обеспечение информационной безопасности бизнеса
11. Организационно-правовые меры обеспечения режима защиты информации
12. Организация информационной безопасности в коммерческом секторе
13. Организация системы безопасности корпоративных информационных систем
14. Защита информации и информационная безопасность финансовых организаций
15. Оценка экономической эффективности системы защиты информации в организации
16. Применение (не)квалифицированной электронной подписи.
17. Анализ деятельности Роскомнадзора в контроле Интернета
18. Защита информации и обеспечение информационной безопасности инфраструктуры центр обработки данных
19. Разработка рекомендаций по повышению эффективности защиты информации в корпоративной сети передачи данных
20. Разработка технического задания на подсистему обеспечения информационной безопасности базовой инфраструктуры катострофо-устойчивости
21. Разработка эскизного проекта системы обеспечения информационной безопасности заданного объекта информатизации
22. Оценка уровня угроз при распространении информации в социальных сетях
23. Регулирование деятельности с применением криптографии в России
24. Информационная безопасность и защита информации в сфере электронной торговли
25. Современные DDoS-атаки (Distributed Denial of Service, распределённая атака типа отказ в обслуживании) как угроза для бизнеса в Интернете: методы и средства защиты
26. Проблемы авторизации субъекта доступа
27. Тенденции развития отечественных средств электронной подписи
28. Анализ инцидентов информационной безопасности в организации
29. Структурирование массива событий и инцидентов информационной безопасности с использованием специализированного программного обеспечения
30. Методы разграничения доступа в компьютерных системах и их правовая регламентация
31. Управление инцидентами информационной безопасности на предприятии
32. Техническое регулирование информационной безопасности в России и за рубежом
33. Обеспечение информационной безопасности и защита информации на предприятиях малого и среднего бизнеса
34. Организационно-технические мероприятия по обеспечению информационной безопасности

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

Не предусмотрено

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Введение				*								
Виды угроз ИБ				*								
Безопасность программного обеспечения				*								
Встроенные средства безопасности операционных систем				*								
Криптографические методы защиты информации				*								
Сетевые средств защиты информации	*	*		*								
Управление рисками ИБ	*	*		*								

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Об информации, информационных технологиях и о защите информации. Федеральный закон № 149-ФЗ от 27.07.2006 (с изменениями и дополнениями) Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/
2. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: уч. пособие. М._Берлин: Директ-Медиа, 2015-253 с. Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=276557
3. Спиричева Н. Р. Алгоритмы блочной криптографии : учебно-методическое пособие для студентов, обучающихся по программе бакалавриата по направлению подготовки 230100 «Информатика и вычислительная техника» / Н. Р. Спиричева; Министерство образования и науки РФ, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. — Екатеринбург : Изд-во Урал, ун-та, 2013. — 78, [2] с. Режим доступа: http://hdl.handle.net/10995/28062

1. Сагдеев К.Н., Петренко В.И., Чипига А.Ф. Физические основы защиты информации; уч. пособие – Ставрополь: Изд-во СКФУ, 2015. – 394 с. Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=458285
4. Долозов Н.Л. Программные средства защиты информации: конспект лекций / Н.Л. Долозов, Т.А. Гультяева. – Новосибирск: Изд-во НГТУ, 2015. – 63 с. Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=438307
5. Скрипник Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. – М.: Национальный открытый университет «ИНТУИТ», 2016. - Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=429070

9.1.2.Дополнительная литература

1. Об электронной подписи. Федеральный закон № 63-ФЗ от 06.04.2011. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/
2. О государственной тайне. Закон РФ № 5485-1 от 21.07.1993 (с изменениями и дополнениями) Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/
3. О коммерческой тайне. Федеральный закон № 98-ФЗ от 29.07.2004 (с изменениями и дополнениями). Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/
4. Закон РФ от 23.09.1992 N 3523-1 (ред. от 02.02.2006) "О правовой охране программ для электронных вычислительных машин и баз данных" http://www.consultant.ru/document/cons_doc_LAW_1007/
5. Указ Президента РФ от 16.08.2004 N 1085 (ред. от 31.12.2015) "Вопросы Федеральной службы по техническому и экспортному контролю" http://www.consultant.ru/document/cons_doc_LAW_14031/
6. Постановление Правительства РФ от 03.02.2012 N 79 (ред. от 15.06.2016) "О лицензировании деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации") http://www.consultant.ru/document/cons_doc_LAW_125798/
7. Постановление Правительства РФ от 03.03.2012 N 171 (ред. от 15.06.2016) "О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации") http://www.consultant.ru/document/cons_doc_LAW_127010/
8. Меры защиты информации в государственных информационных системах http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument

9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god
10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god
11. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (части 1, 2, 3) http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/381-rukovodyashchij-dokument
12. Руководящий документ. Защита от несанкционированного доступа к информации Часть 1. http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/382-rukovodyashchij-dokument-prikaz-predsedatelya-gostekhkomissii-rossii-ot-4-iyunya-1999-g-n-114
13. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g
14. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g
15. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2
16. Защита от несанкционированного доступа к информации. Термины и определения http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3
17. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/387-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g4
18. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования http://fstec.ru/component/attachments/download/316
19. Информационное сообщение об утверждении методических документов, содержащих профили защиты межсетевых экранов http://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1184-informatsionnoe-soobshchenie-fstek-rossii-ot-12-sentyabrya-2016-g-n-240-24-4278
20. Аверченков В.И. Защита персональных данных в организации / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. – 3-е изд., стереот. – М.: ФЛИНТА, 2016. – 124 с. Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=93260
21. Сергеева Ю.С. Защита информации. Конспект лекций. Учебное пособие / Сергеева Ю. С. — Москва :А-Приор, 2011.—128.— Режим доступа: :http://www.biblioclub.ru/index.php?page=book&id=72670
22. Шеннон К. Теория связи в секретных системах. / В кн. Лекции по теории информации и кибернетике.–М.: ИЛ, 1963. - Режим доступа: http://www.enlight.ru/crypto/articles/shannon/shann__i.htm

23. Аверченков В.И. Система защиты информации в ведущих зарубежных странах.: уч. пособие / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашкин, М.В. Рудановский. – 4-е изд., стереотип. – М.: ФЛИНТА, 2016. – 224 с. Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=93351
24. Аверченков В.И. Служба защиты информации: организация и управление: уч. пособие / В.И. Аверченков, М.Ю. Рытов. – 3-е изд., стереотип. – М.: ФЛИНТА, 2016. – 186 с. Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=93356
25. Аверченков В.И. Аудит информационной безопасности: уч. пособие / В.И. Аверченков. –3-е изд., стереотип. – М.: ФЛИНТА, 2016. – 269 с. Режим доступа: http://biblioclub.ru/index.php?page=book_view_red&book_id=93245

9.2.Методические разработки

Не используются

9.3.Программное обеспечение

Математические пакеты:
Mathcad, математический пакет MatLab, MS Excel.

Sage - https://ru.wikipedia.org/wiki/Sage http://www.sagemath.org http://www.sagemath.org/ru/
PARI/GP - https://en.wikipedia.org/wiki/PARI/GP https://pari.math.u-bordeaux.fr
OpenSSL - https://www.openssl.org https://ru.wikipedia.org/wiki/OpenSSL
http://gnuwin32.sourceforge.net/packages/openssl.htm

Операционные системы:
Kali Linux - https://ru.wikipedia.org/wiki/Kali_Linux https://www.kali.org
NST - Network Security Toolkit (NST) is a Linux-based Live DVD/USB
http://www.networksecuritytoolkit.org/nst/index.html
https://en.wikipedia.org/wiki/Network_Security_Toolkit

Среда программирования:
Python - https://ru.wikipedia.org/wiki/Anaconda_(дистрибутив_Python)
https://www.anaconda.com/what-is-anaconda/ https://ipython.org/notebook.html
Perl - https://www.cpan.org https://ru.wikipedia.org/wiki/CPAN https://ru.wikipedia.org/wiki/Perl

9.4. Базы данных, информационно-справочные и поисковые системы

http://www.iso.org/ Международные стандарты безопасности ISO
http://fstec.ru/ Федеральная служба по техническому и экспортному контролю
www.consultant.ru – справочная система «Консультант-Плюс»;
www.garant.ru – справочная система «Гарант»;
http://window.edu.ru – единое окно доступа к образовательным ресурсам

9.5.Электронные образовательные ресурсы

Не используются

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Аудитории для проведения занятий, оснащенные мультимедийными средствами; компьютерные классы; демонстрационные материалы. ПК для преподавателя и студентов с доступом в Интернет.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины – 1 *утверждается ученым советом института*], в том числе, **коэффициент значимости курсовых работ/проектов, если они предусмотрены –0.**

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,4		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение лекций	7, 1-17	*20*
Конспект лекций	7, 1-17	*20*
Домашняя работа 1	7, 1-17	*60*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,5 **Промежуточная аттестация по лекциям –** *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,6		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Активность на практиках	7, 1-17	60
Домашняя работа 2	7, 1-17	40
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям– *нет* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 7	**1**

*В случае проведения промежуточной аттестации по дисциплине (экзамена, зачета) методом тестирования используются официально утвержденные ресурсы: АПИМ УрФУ, СКУД УрФУ, имеющие статус ЭОР УрФУ; ФЭПО (www.фэпо.рф); Интернет-тренажеры (www.i-exam.ru).

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

- в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
- при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

Не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Концепция информационной безопасности.
2. Виды угроз. Внутренние и внешние источники угроз.
3. Организационно-правовое обеспечение информационной безопасности.
4. Угрозы в информационных системах.
5. Способы защиты информации.
6. Средства защиты информации.
7. Компьютерные вирусы и антивирусные программы.
8. Государственные стандарты по информационной безопасности.
9. Понятие информационной безопасности. Угрозы. Механизмы анализа угроз. Инструментарий построения рубежей.
10. Основы криптографии. Шифрование и кодирование. Общие принципы и модели.
11. Защита от несанкционированного доступа.
12. Простые шифры. Шифр простой замены. Шифр Цезаря (шифр сдвига, код Цезаря, сдвиг Цезаря).
13. Шифр вертикальной перестановки (перестановочный шифр, шифрограмма по вертикалям).
14. Гаммирование (метод симметричного шифрования).
15. Методы расшифровки зашифрованной информации. Основные способы криптоанализа простых шифров.
16. Основные методы криптоанализа. Атака на основе шифротекста, открытых текстов и соответствующих шифротекстов, подобранного открытого текста, адаптивно подобранного открытого текста.
17. Дополнительные методы криптоанализа. Атака на основе подобранного шифротекста, подобранного ключа. Бандитский криптоанализ
18. Симметричные криптосистемы. Схема, сеть Фейстеля (Horst Feistel, Feistel network, Feistel cipher). Стандарты блочного шифрования. Федеральный стандарт DES.
19. Симметричные криптосистемы. Алгоритм шифрования ГОСТ 28147-89 (Магма), ГОСТ Р 34.12-2015 (Кузнечик). режимы шифрования и гаммирования.

20. Симметричные криптосистемы. Алгоритм блочного шифрования Rijndael - Advanced Encryption Standard (AES).
21. Атаки на блочные шифры. Дифференциальный криптоанализ. Дифференциальный криптоанализ на основе отказов устройства.
22. Атаки на блочные шифры. Линейный криптоанализ. Силовая атака на основе распределенных вычислений.
23. Поточные шифры. Регистры сдвига с обратной связью. Алгоритм поточного шифрования RC4 (Rivest cipher 4, Ron's code; ARC4, ARCFOUR).
24. Основные теоремы теории чисел. Проверка числа на простоту. Эффективные алгоритмы возведения в степень.
25. Криптосистема RSA (Rivest-Shamir-Adleman — криптографический алгоритм с открытым ключом). Устройство RSA. Эффективность реализации. Криптостойкость RSA.
26. Атаки на криптосистему RSA. Атака на основе выбранного шифр текста. Атака на основе общего RSA модуля. Раскрытие малого показателя шифрования.
27. Криптосистема Эль-Гамаля (Elgamal). Вычисление и проверка подписи. Шифрование и дешифрование. Эффективность реализации.
28. Метод экспоненциального ключевого обмена Диффи-Хелмана. Протокол ключевого обмена для нескольких участников.
29. Хеш-функции. Понятие хеш-функции. Основные свойства односторонних функций. MD4 (Message Digest 4), RFC 1186 (The MD4 Message Digest Algorithm).
30. Цифровая подпись. Понятие цифровой подписи. Основные принципы и отличия от реальной подписи. Алгоритмы цифровой подписи - ГОСТ Р 34.10-2012. DSS (Digital Signature Standard).
31. Закон об электронной цифровой подписи в России. Удостоверяющие центры.
32. Протоколы генерации ключей. Случайные ключи. Протоколы распределения ключей.
33. Разделение секрета. Схема разделения секрета Шамира.
34. Применение помехоустойчивых кодов в криптографии. Недвоичные циклические коды Рида-Соломона(Reed–Solomon codes).
35. Верифицируемое разделение секрета.
36. «Шарады» с временным замком (Time-lock puzzles and timed-release Crypto). Построение «шарад» с временным замком. Решение «Шарады»
37. Квантовая криптография - основанная на принципах квантовой физики. Квантовый протокол распределения ключей. Распределение ключей в оптических сетях.
38. Криптографические протоколы: обеспечение различных режимов аутентификации; генерация, распределение и согласование криптографических ключей; защита взаимодействий участников; разделение ответственности между участниками.
39. Доказательство принадлежности (Zero-knowledge proof). Доказательство при отказе отправителя. Доказательство при отказе получателя.
40. Нормативно-правовое обеспечение информационной безопасности.
41. Классификация секретной информации в России. Служебная, коммерческая и государственная тайны.
42. Законы РФ: «Информации, информатизации и защите информации»; Закон о персональных данных
43. Стандарты ИБ: ISO/IEC 15408; руководящие документы ФСТЭК; Оранжевая книга (Критерии определения безопасности компьютерных систем - Trusted Computer System Evaluation Criteria; Радужная серия).
44. Политика безопасности. Уровень гарантированности. Классы безопасности. Безопасность распределенных систем. Рекомендации X.800.
45. Роли и ответственности субъектов информационного пространства. Принцип распределения ответственности. Матрица распределения доступа для сотрудников организации.
46. Понятие управления рисками. Качественные и количественные методики оценки рисков. Количественная модель рисков QRM (Quantitative Risk Model). Оценки по конфиденциальности информации.

47. Политика информационной безопасности. Цели и задачи организации. Взаимодействие между субъектами. Правила безопасности.
48. Политика информационной безопасности для локальной вычислительной сети.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено

8.3.9. Примерные требования и задания для домашней работы

Студентам предлагается подготовить и сделать доклад (в виде презентации) по выбранной теме.
Объем работы задается временем, отводимым на презентацию – до 10 минут.
Примерная тематика докладов приведена в п. 4.3.1